68 erfolgreiche Ransomware-Angriff auf Unternehmen 2023

- BSI Lagebericht 2023

„206 Milliarden Euro Schaden ist den Unternehmen in Deutschland in den vergangenen zwölf Monaten durch Wirtschaftskriminalität entstanden, davon rund 150 Milliarden Euro durch Cyberattacken“

– Bitkom zum BSI-Jahresbericht 2023

„Die Bedrohung im Cyberraum ist so hoch wie nie zuvor“

- BSI Lagebericht 2023

„Das ITSiG fordert von KRITIS-Betreibern die Einhaltung oder mindestens Berücksichtigung des „Standes der Technik“ von IT-Sicherheitsmaßnahmen. Dieses Sicherheitsniveau wird im Gesetz allerdings nicht weitergehend konkretisiert.“

- TeleTrusT Stand der Technik in der IT-Sicherheit

Der Maschinebau ist die am stärksten betroffene Branche des NIS2 in Deutschland mit rund 3600 Maschinen und Anlagenbauern. Dies sind 58% der gesamten Branche und 75% davon sind KMU.

- VDMA Diskussionspapier zum Referentenentwurf des NIS2UmsuCG

Verteidigung der Master-Thesis

Erstellung eines Umsetzungsleitfaden informationstechnischer Sicherheitsmaßnahmen für Maschinen anhand der IEC-62443

Max-Florian Beck

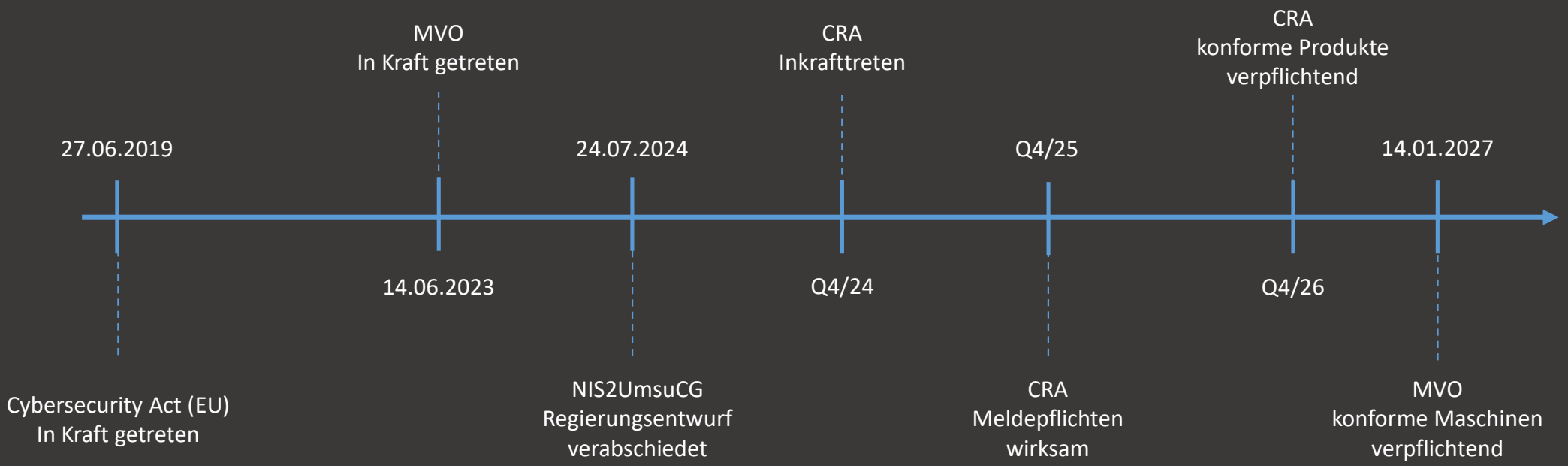
Studiengang: IT-Sicherheit und Forensik

HOCHSCHULE WISMAR
UNIVERSITY OF APPLIED SCIENCES TECHNOLOGY, BUSINESS AND DESIGN

Gliederung

- Rechtliche und Normative Grundlagen
- Anforderungsanalysen
- Erstellung der Kataloge
- Durchführung des IEC-62443-3-2 Cyber Security Risikobewertungsprozess
- Erstellung des Abnahmeprotokolls
- Validierung durch externes Fachpersonal

Entwicklung der Informationssicherheit in DE



Europäischer Rechtsakt zur Cybersicherheit

- Seit 27.06.2019 in Kraft (Verordnung (EU) 2019/881)
- Stärkung der ENISA (permanentes Mandat)
- Einführung einheitlicher europäischer Cybersicherheitszertifizierungen (EUCC)
- Soll harmonisierend sein.
  Ein EUCC nach Verordnung (EU) 2019/881 dient als Nachweis zur Erfüllung aller EU-Regulatorien (NIS2, CRA, MVO)

NIS2Umsetzungs- und Cybersicherheitsstärkungsgesetz

- Vsl. Oktober/2024 in Kraft
- Dient dazu EU-weite Mindestanforderungen für Cybersecurity festzulegen
- Konkrete Vorgaben von Verpflichtungen und Umsetzungen
- Nichteinhaltung führt zu Bußgeldern
- Betrifft direkt IT, indirekt OT

Einordnung der Kategorien

- Eingruppierung der Wirtschaftsakteure in 3 Kategorien

Einrichtung	Größe	Rahmenbedingung	Sektoren
Besonders wichtig § 28 Abs. 1	Groß-unternehmen aus Anlage 1	> 249 Mitarbeiter oder Jahresumsatz von 50 Mio. € und Jahresbilanz-summe von > 43 Mio. €	Energie, Transport/Verkehr, Finanzen/Versicherungen, Gesundheit, Wasser/Abwasser, IT und TK, Weltraum
	Mittlere TK Unternehmen	> 49 Mitarbeiter oder Jahresumsatz und Jahresbilanzsumme von > 10 Mio. €	Anbieter öffentlicher TK-Netze und TK-Dienste
	Unabhängig	Keine	Qualifizierte Vertrauendienste, TLD-Registries, DNS-Dienste, Betreiber kritischer Anlagen (KRITIS-Betreiber)
Wichtig § 28 Abs. 2	Mittlere Unternehmen aus Anlage 1 Unternehmen aus Anlage 2	> 49 Mitarbeiter oder Jahresumsatz und Jahresbilanzsumme von > 10 Mio. €	Energie, Transport/Verkehr, Finanzen/Versicherungen, Gesundheit, Wasser/Abwasser, IT und TK, Weltraum, Post/Kurier, Siedlungsabfallentsorgung, Chemie, Lebensmittel, Verarbeitendes Gewerbe, Digitale Dienste, Forschung
	Unabhängig	Keine	Vertrauensdienstanbieter
Bundes-verwaltung § 29	Stellen des Bundes, Körperschaften, Anstalten, Stiftungen des öffentlichen Rechts sowie ihre Vereinigungen, öffentliche Unternehmen die mehrheitlich im Eigentum des Bundes stehen und die IT-Dienstleistung für die Bundesverwaltung erbringen - die keine Institution der sozialen Sicherung sind		

Eigene Darstellung nach „Das NIS2-Umsetzungsgesetz NIS2UmsuCG – OpenKRITIS“ Kapitel: Einrichtungen

Herausforderungen des Maschinenbaus

- Doppelte Betroffenheit (IT/OT)
- Kunden sind oftmals große Betreiber (wesentliche Einrichtungen) wodurch Anforderungen delegiert werden
- In der OT hauptsächlich Legacy Systeme / Neu-Systeme nach wie vor nicht auf dem IT-Stand
- Bisherige Zertifizierungen werden möglicherweise hinfällig

https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html

Cyber Resilience Act (CRA)

- Vsl. Q4/2024 in Kraft
- Erhöhung der Cybersicherheit von digitalen Produkten im gesamten europäischen Wirtschaftsraum
- Digitales Produkt betrifft sowohl Hardware als auch Software
- Nichteinhaltung führt zu Bußgeldern

Einordnung der Produkte

- So gut wie alle Industrie-Komponenten
- Bisher keine „Anforderungsunterscheidung“ zwischen Klasse 1 und 2
- Soll durch zusätzliche, kommende Rechtsakte geregelt werden

Kategorie	Betroffene Produkte
Maschinenbau-relevante Produkte der Klasse 1	Software für Identitätsmanagementsysteme und Software für die Verwaltung des privilegierten Zugangs, eigenständige und eingebettete Browser, Passwort-Manager, Software für die Suche/Entfernung/Quarantäne von Schadsoftware, Produkte mit digitalen Elementen mit der Funktion eines virtuellen privaten Netzes (VPN), Netzmanagementsysteme, Instrumente für die Netzkonfigurationsverwaltung, Systeme für die Überwachung des Netzverkehrs, SIEM-Systeme, Aktualisierungs- und Patchverwaltung, Software für Fernzugriff und gemeinsame Datennutzung, physische Netzschnittstellen, IACS und IIoT-Geräte, FPGAs für Einrichtungen gemäß Anhang 1 der NIS2
Maschinenbau-relevante Produkte der Klasse 2	Public-Key-Infrastrukturen und Aussteller digitaler Zertifikate, Firewalls/ Angriffs- und/oder -präventionssysteme für den industriellen Einsatz, Allzweck-Mikroprozessoren, Mikroprozessoren die für die Integration in speicherprogrammierbare Steuerungen und Sicherheitselemente bestimmt sind, Router, Modems für die Internetanbindung, Switche für den industriellen Einsatz, Sicherheitselemente, Hardware-Sicherheitsmodule, sichere Kryptoprozessoren, Chipkarten, Chipkartenleser, Token, IACS, IIoT-Geräte, Sensor- und Aktuatorkomponenten von Robotern und Robotersteuerungen

Eigene Darstellung nach Anhang 3 in „COM(2022) 454 final, 2022/0272(COD)“ der Europäischen Kommission

Herausforderungen

- Erhöhte Dokumentationspflicht
- Hohe Heterogenität führt zu Unübersichtlichkeiten
- Unklare Kommunikationswege und Verantwortlichkeiten
- Fachkräftemangel

https://www.dihk.de/de/themen-und-positionen/wirtschaft-digital/dihk-durchblick-digital/cyber-resilience-act-cra--90956

Maschinenverordnung (MVO)

- Seit 06/2023 in Kraft und ab 01/2027 geltend
- Regelt das Inverkehrbringen von Maschinen im gesamten europäischen Wirtschaftsraum
- Schwerpunkt auf funktionaler Sicherheit, Cyber Security nun aber ebenfalls fester Bestandteil zur rechtmäßigen Funktionsfähigkeit der Safety
- 2 Unterkapitel für Cyber Security – Anhang 3 Abschnitt 1.1.9 und 1.2.1

Normative Grundlagen

- IEC-62443, Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme, ist die führende Norm im Bereich Industrielle Cyber Security

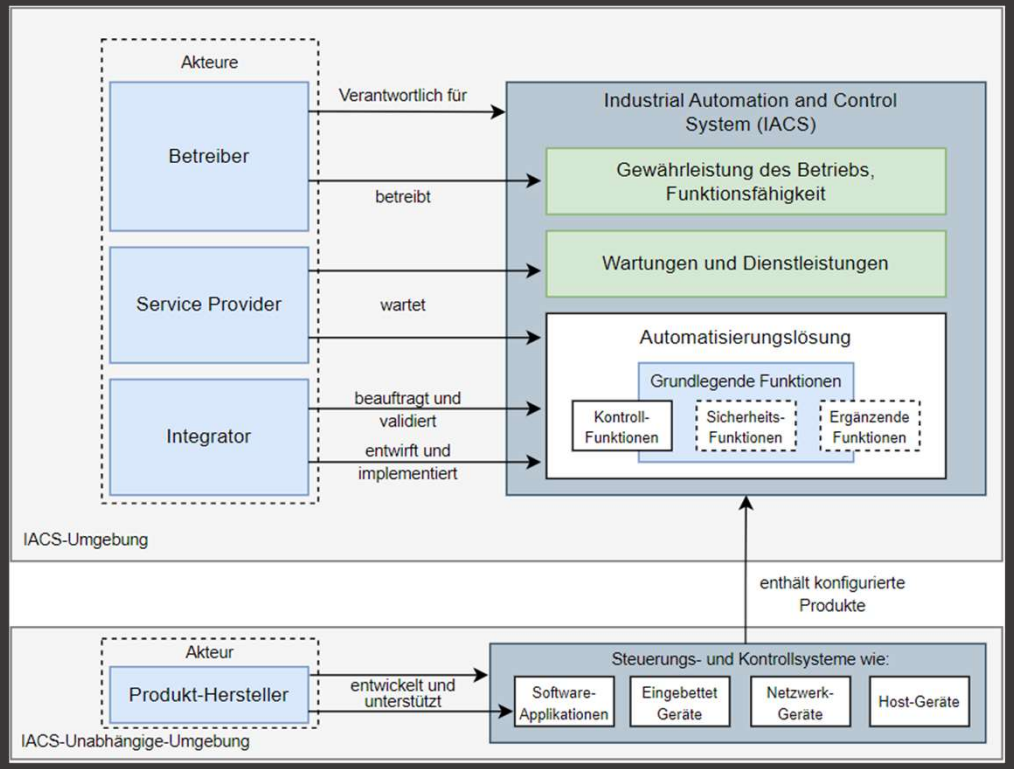
- Besteht aus 4 Teilen:
  - Allgemein
  - Richtlinien und Prozeduren
  - System
  - Produkt

- Relevant sind alle Teile außer Produkt

IEC-62443

- Definiert 4 Wirtschaftsakteure:
  - Betreiber
  - Integratoren
  - Produkt-Hersteller
  - Service-Provider

- Maschinenbauer gelten als Integratoren und in gewissen Fällen auch als Service-Provider



Eigene Darstellung nach „Overview of ISA/IEC 62443 for Product Suppliers, IC46, Version 1.0, ISA-Trainingsunterlagen, S.40

Kernprinzipien

- Foundational Requirements – 7 Grundanforderungen als Erweiterung des CIA-Modells
- Defense in Depth – Zentrale Sicherheitsarchitektur nach dem Zwiebelschalenmodell
- Zones & Conduits – Zonierung der Systeme
- Security Level – Klassifizierung der Robustheit von Systemen
- Cyber Security Management System – Steuerung, Überwachung und Bewertung der Cyber Security innerhalb des Unternehmens

Anforderungsanalyse

- Rechtliche Anforderungen an Maschinenbauer
- Normative Anforderungen der System Requirements
- Prüfung der gesetzlichen Konformität der IEC-62443

Rechtliche Anforderungen an Maschinenbauer

- Aufteilung in 2 Überkategorien:
  - Kommunikationspflichten – Maschinenbauer muss Informationen weitergeben, bereithalten oder bereitstellen
  - Handlungspflichten – Maschinenbauer muss aktiv Maßnahmen treffen

- Weitere Unterteilung in konkrete Pflichten.

- Beachtet wurden NIS2UmsuCG, CRA und MVO

Rechtliche Anforderungen an die OT der Maschinenbauer

Kommunikationspflichten			
Meldepflicht	Unterrichtungspflicht	Nachweispflicht	Kennungspflicht
§11 Abs. 1 CRA	§10 Abs. 14 CRA	§10 Abs. 3 CRA	Anhang 3 Teil B Absatz 1.1.9. MVO
§11 Abs. 2 CRA		§10 Abs. 5 CRA	
§11 Abs. 4 CRA		§10 Abs. 7 CRA	
§11 Abs. 7 CRA		§10 Abs. 8 CRA	
		§10 Abs. 9 CRA	
		§10 Abs. 10 CRA	
		§10 Abs. 11 CRA	
		§10 Abs. 13 CRA	
		§17 Abs. 1 CRA	
		§17 Abs. 2 CRA	
		Anhang 3 Teil B Absatz 1.2.1 MVO	

Eigene Darstellung

Handlungspflichten				
Prüfungspflicht	Korrekturpflicht	Rückrufpflicht	Umsetzungspflicht	Kooperationspflicht
§10 Abs. 2 CRA	§10 Abs. 6 CRA	§10 Abs. 12 CRA	Anhang 3 Teil B Absatz 1.1.9. MVO	§10 Abs 13 CRA
§10 Abs. 4 CRA	§10 Abs. 12 CRA		Anhang 3 Teil B Absatz 1.2.1 MVO	
			§10 Abs. 1 CRA	
			§10 Abs. 2 CRA	
			§10 Abs. 6 CRA	

Eigene Darstellung

Normative Anforderungen an Maschinenbauer

Accountmanagement	Identifikationsmanagement	Systemsicherheit	Netzwerkmanagement	Auditierungsmanagement	Ressourcenmanagement
SR 1.3	SR 1.1	SR 2.3	SR 1.13	SR 2.8	SR 5.4
SR 1.4	SR 1.1 RE 1	SR 2.4	SR 1.13 RE 1	SR 2.9	SR 7.1
SR 1.5	SR 1.2	SR 3.2	SR 2.6	SR 2.10	SR 7.1 RE 1
SR 1.7		SR 3.2 RE 1	SR 5.1	SR 2.11	SR 7.2
SR 1.8	Drahtlose Kommunikation	SR 3.3	SR 5.1 RE 1	SR 3.4	SR 7.8
SR 1.9	SR 1.6	SR 3.5	SR 5.2	SR 3.9	
SR 1.10	SR 1.6 RE 1	SR 3.6	SR 5.2 RE 1	SR 6.1	Kommunikationssicherheit
SR 1.11	SR 2.2	SR 3.7	SR 5.3	SR 6.2	SR 3.1
SR 2.1		SR 4.2	SR 7.6		SR 4.1
SR 2.1 RE 1	Sitzungsmanagement	SR 7.3	SR 7.7		SR 4.1 RE 1
SR 2.1 RE 2	SR 1.12	SR 7.3 RE 1			SR 4.3
	SR 2.5	SR 7.4			
	SR 3.8	SR 7.5			

Eigene Darstellung

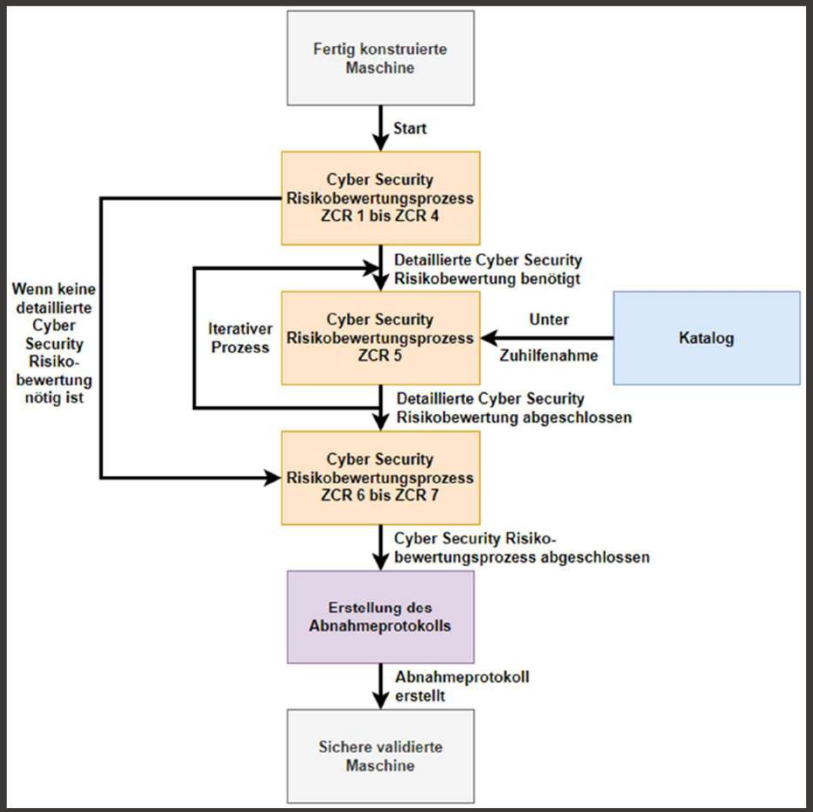
Prüfung der gesetzlichen Konformität der IEC-62443

- Kennungspflicht
  - Erfüllt durch CRS
- Unterrichtungspflicht
  - Nicht erfüllt
- Meldepflicht
  - Nicht erfüllt, CRS bietet Grundlage
- Nachweispflicht
  - Nicht erfüllt, CRS bietet Grundlage
- Prüfungspflicht
  - Nicht erfüllt
- Korrekturpflicht
  - Erfüllt durch Cyber Security Lifecycle
- Rückrufpflicht
  - Nicht Erfüllt
- Kooperationspflicht
  - Nicht Erfüllt
- Schulungspflicht
  - Erfüllt durch CSMS
- Umsetzungspflicht
  - Erfüllt durch Cyber Security Risikobewertungsprozess, SRs, CRS

Umsetzungsleitfaden als Unterstützung

- Bietet ein vorgehen zur Umsetzung der Risikobewertung in Verbindung mit Dokumentationen

- Kataloge Unterstützen den Vorgang



Eigene Darstellung

https://umsetzungsleitfaden.gitbook.io/leitfaden-zur-erhohung-der-security-von-maschinen

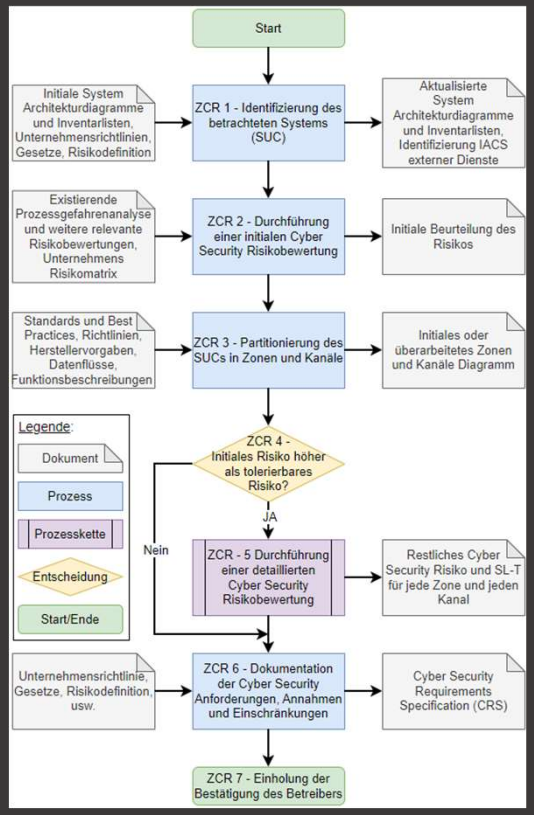
Erstellung der Kataloge

- Kataloge zur Umsetzungsunterstützung
- Maßnahmen Kataloge (Organisatorisch und Technisch)
- Prüftools und –verfahren Katalog
- Bedrohungskatalog
- Grundlegender Katalog

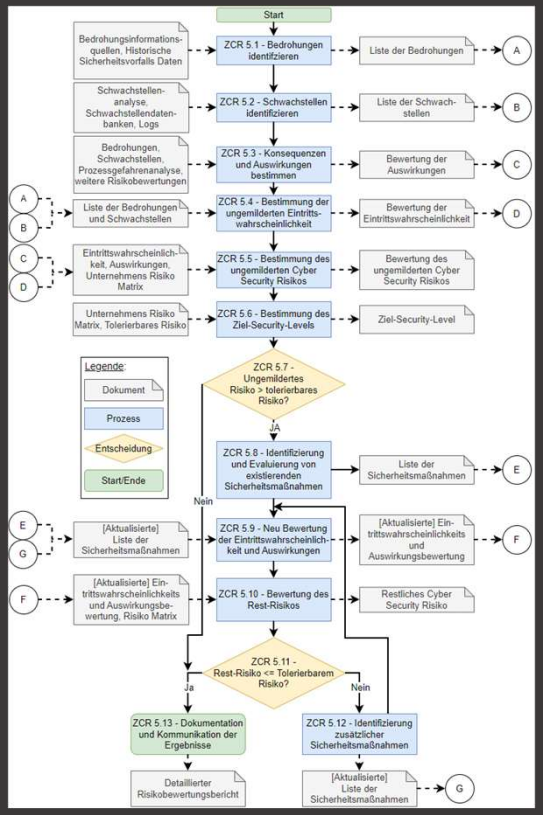
Cyber Security Risikobewertungsprozess

- Risikobasierte Bewertung der Sicherheit eines Systems
- Rechtlich notwendig durch § 10 Abs. 2 CRA
- Dokumentierte Durchführungsschritte zur Unterstützung
- Cyber Security Requirements Specification als Dokumentationsunterstützung

Cyber Security Risikobewertungsprozess

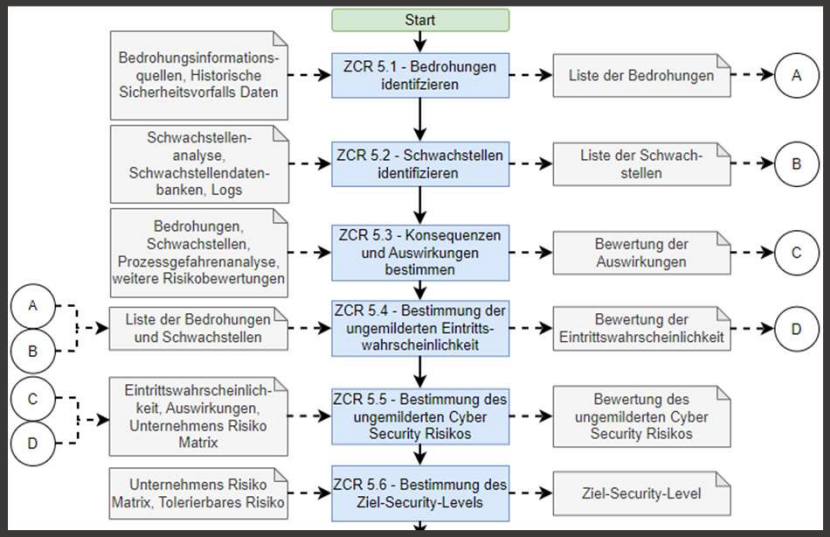


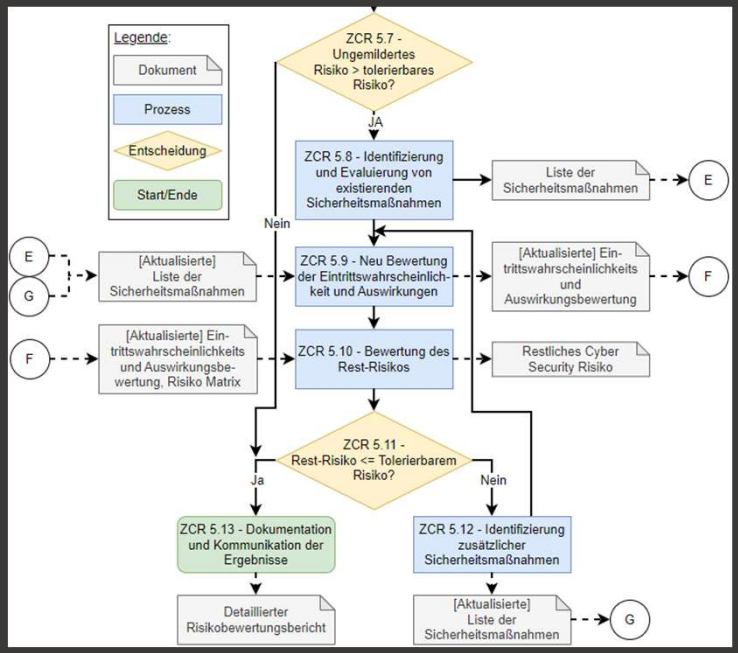
Eigene Darstellung nach IEC-62443-3-2-2020 Seite 18



Eigene Darstellung nach IEC-62443-3-2-2020 Seite 23

Cyber Security Risikobewertungsprozess



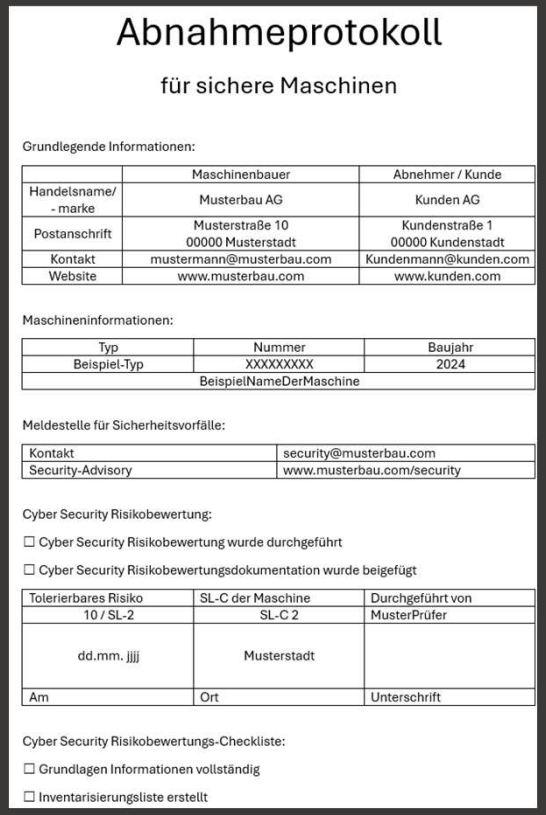


Eigene Darstellung nach IEC-62443-3-2-2020 Seite 23

Erstellung des Abnahmeprotokolls (Erweiterte CRS)

- Allgemeine Informationen (Kunde, Maschine, Land, usw.)
- Maschinendokumente (Netzplan, Inventarisierungsliste, Softwareversionen, …)
- Implementierte Maßnahmen nach Katalog
- Dokumentation der Prüfungen
- Bestimmung des erreichten Sicherheitslevels

Erstellung des Abnahmeprotokolls (Erweiterte CRS)



Abnahmeprotokoll

für sichere Maschinen

Grundlegende Informationen:

	Maschinenbauer	Abnehmer / Kunde
Handelsname/ - marke	Musterbau AG	Kunden AG
Postanschrift	Musterstraße 10 00000 Musterstadt	Kundenstraße 1 00000 Kundenstadt
Kontakt	mustermann@musterbau.com	Kundenmann@kunden.com
Website	www.musterbau.com	www.kunden.com

Maschineninformationen:

Typ	Nummer	Baujahr
Beispiel-Typ	XXXXXXXXX	2024
BeispielNameDerMaschine		

Meldestelle für Sicherheitsvorfälle:

Kontakt	security@musterbau.com
Security-Advisory	www.musterbau.com/security

Cyber Security Risikobewertung:

☐ Cyber Security Risikobewertung wurde durchgeführt

☐ Cyber Security Risikobewertungsdokumentation wurde beigefügt

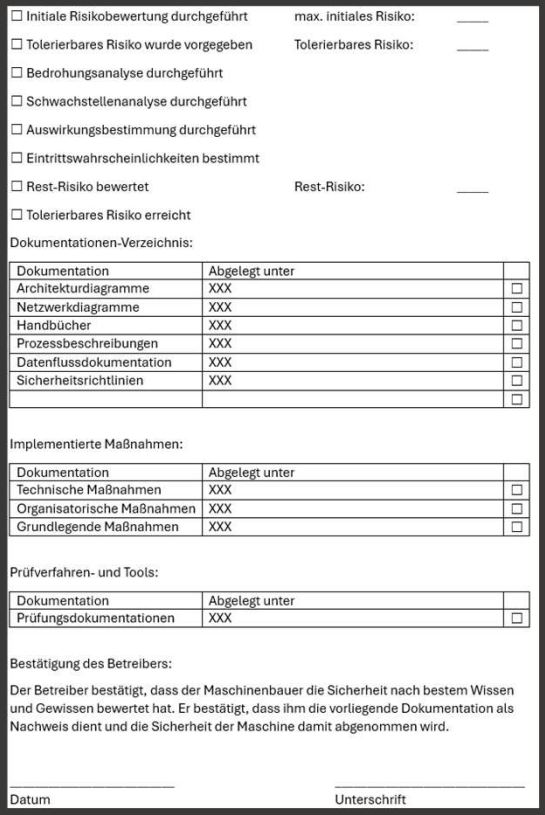
Tolerierbares Risiko	SL-C der Maschine	Durchgeführt von
10 / SL-2	SL-C 2	MusterPrüfer
dd.mm. jjjj	Musterstadt	
Am	Ort	Unterschrift

Cyber Security Risikobewertungs-Checkliste:

☐ Grundlagen Informationen vollständig

☐ Inventarisierungsliste erstellt

Eigene Darstellung



☐ Initiale Risikobewertung durchgeführt max. initiales Risiko: ____

☐ Tolerierbares Risiko wurde vorgegeben Tolerierbares Risiko: ____

☐ Bedrohungsanalyse durchgeführt

☐ Schwachstellenanalyse durchgeführt

☐ Auswirkungsbestimmung durchgeführt

☐ Eintrittswahrscheinlichkeiten bestimmt

☐ Rest-Risiko bewertet Rest-Risiko: ____

☐ Tolerierbares Risiko erreicht

Dokumentationen-Verzeichnis:

Dokumentation	Abgelegt unter	
Architekturdiagramme	XXX	☐
Netzwerkdiagramme	XXX	☐
Handbücher	XXX	☐
Prozessbeschreibungen	XXX	☐
Datenflussdokumentation	XXX	☐
Sicherheitsrichtlinien	XXX	☐
		☐

Implementierte Maßnahmen:

Dokumentation	Abgelegt unter	
Technische Maßnahmen	XXX	☐
Organisatorische Maßnahmen	XXX	☐
Grundlegende Maßnahmen	XXX	☐

Prüfverfahren- und Tools:

Dokumentation	Abgelegt unter	
Prüfungsdokumentationen	XXX	☐

Bestätigung des Betreibers:

Der Betreiber bestätigt, dass der Maschinenbauer die Sicherheit nach bestem Wissen und Gewissen bewertet hat. Er bestätigt, dass ihm die vorliegende Dokumentation als Nachweis dient und die Sicherheit der Maschine damit abgenommen wird.

Datum Unterschrift

Eigene Darstellung

Validierung durch externes Fachpersonal

- Interview mit Dr.-Ing. Christian Haas
- Gruppenleiter für Industrielle Cybersicherheit am Fraunhofer IOSB
- Konnte die Herausforderungen des Maschinenbaus bestätigen
- Hat den Risikobewertungsprozess nach IEC-62443-3-2 empfohlen
- Begrüßt den Umsetzungsleitfaden

Literatur

1. Bundesamt für Sicherheit in der Informationstechnik (BSI), „Die Lage der IT-Sicherheit in Deutschland 2023," Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2023
2. ANSI/ISA-62443-1-1 (99.01.01)-2007, „Security for industrial automation and control systems; Part 1-1: Terminology, Concepts, and Models"; ISBN: 978-1-934394-37-3
3. ANSI/ISA-62443-3-2-2020, „Security for industrial automation and control systems; Part 3-2: Security risk assessment for system design"; ISBN: 978-1-64331-116-6
4. ANSI/ISA-62443-3-3 (99.03.03)-2013, „Security for industrial automation and control systems; Part 3-3: System security requirements and security levels"; ISBN: 978-0-876640-39-5
5. Bundeskriminalamt, „Cybercrime. Bundeslagebild 2023," Bundeskriminalamt, Wiesbaden, 2023
6. Bitkom e.V., „Bitkom zum Bundeslagebild Cybercrime," Bitkom e.V., 13 Mai 2024. [Online]. Available: https://www.bitkom.org/Presse/Presseinformation/Statement-Bundeslagebild-Cybercrime. [Zugriff am 16 August 2024]
7. TeleTrusT „Stand der Technik in der IT-Sicherheit". [Online] Available: https://www.teletrust.de/publikationen/broschueren/stand-der-technik/ [Zugriff am 15 August 2024]
8. OpenKRITIS, „NIS2 Umsetzungsgesetz," OpenKRITIS, [Online]. Available: https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html. [Zugriff am 19 August 2024]
9. S. Zimmermann, „NIS2UmsuCG - VDMA-Stellungnahme zum Diskussionspaper des BMI zur Umsetzung der NIS2-Richlinie in Deutschland," 2023. [Online]. Available: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/nis2umsucg.html. [Zugriff am 19 August 2024]
10. Deutsche Industrie und Handelskammer, „Cyber Resilience Act (CRA)," Deutsche Industrie und Handelskammer, [Online]. Available: https://www.dihk.de/de/themen-und-positionen/wirtschaft-digital/dihk-durchblick-digital/cyber-resilience-act-cra--90956. [Zugriff am 19 August 2024].